Cybersecurity and Digital Trade: Pathways for the EU and India

Meghna Bal

FRIEDRICH EBERT STIFTUNG

KOAN

Cybersecurity and Digital Trade: Pathways for the EU and India

Meghna Bal

August 2024

Contents

Foreword

To understand where the EU and India stand on issues of digital trade, the Friedrich-Ebert-Stiftung and Koan Advisory conducted a series of roundtable discussions between stakeholders from both jurisdictions. The second of these discussed stakeholder views on issues in cybersecurity. This paper synthesises views from the second discussion.

List of Abbreviations

EU	European Union
AI	Artificial Intelligence
API	Application Programming Interface
VLOP	Very Large Online Platform
CERT-IN	Indian Computer Emergency Response Team
UN	United Nations
ICT	Information and Communication Technologies
OEWG	Open-ended Working Group
GGE	Group of Governmental Experts
SMEs	Small and Medium-sized Enterprises
US CLOUD	United States Clarifying Lawful Overseas Use of Data Act

List of Figures

Part I. Introduction

Digital trade and cybersecurity are inextricably linked. As data flows become more pervasive, both within and across borders, countries must undertake measures to secure these information channels from different kinds of threats. In recent digital trade chapters, provisions focused on balancing the facilitation of digital trade with the protection of consumer rights and essential security interests.[1] For instance, the United States-Mexico-Canada Trade Agreement encourages reliance on standards based on consensus and best practices in risk management to recognize and safeguard against cybersecurity threats, as well as to detect, respond to, and recover from cybersecurity incidents. However, as the world becomes increasingly polarized across ideological lines, the interplay of digital trade and cybersecurity becomes more complex as it expands to restrictions on certain actors, and increased emphasis on trusted digital supply chains.

With this context in mind, we put together a roundtable on cybersecurity in our series regarding digital trade cooperation between the European Union and India. This paper is a synthesis of the roundtable discussion on cybersecurity and trade.

Part II. Where Germany/European Union Stand on Cybersecurity and Trade

a. Digital Sovereignty

Our discussions revealed that the EU links cybersecurity conversations very closely with a broader digital sovereignty agenda. Digital sovereignty connotes "control of data, software (e.g. AI), standards and protocols (e.g. 5G, domain names), processes (e.g. Cloud computing), hardware, services, and infrastructure". According to Floridi (2019) the term digital sovereignty encapsulates the impulse within European nations to reduce their reliance on Chinese and American companies in the digital realm.[2]

The need for such a policy has been driven home by several episodes. For instance, during COVID, Italy and Germany's attempts at building centralized COVID applications that were not based on the Google-Apple APIs, and would give domestic authorities control over health data, failed.[3] Consequently, both countries had to change course and accept building a decentralized application supported by these two companies.[4] This gave Apple and Google power over what were national applications.[5]

b. Social Media

Another important consideration for the Europeans is the security concern presented by the proliferation of social media, controlled largely by American (Meta, Twitter) and Chinese companies (Tiktok). A study by Kubler et al (2021) found that at least 6.72 percent of posts related to the German election on Facebook and 5.63 percent of election-related tweets could be categorized as illegal, disinformation, or infringing electoral rights.[6]

According to Carrapico and Farrand (2020) social media has taken centre-stage in Europe's security-focussed initiatives largely due to the expansion of Russia's disinformation campaigns that focused on the "destabilization of Europe in 2014" coupled with its "incursions into Ukraine".[7] As far back as 2015, the European Council expressed its concerns on online disinformation, calling for the creation of a targeted action plan. More recently, it passed the Digital Services Act, which among other things, has been introduced to fight online disinformation (European Commission 2023).[8]

The Digital Services Act requires services it deems as "Very Large Online Platforms" (VLOPs) to undertake risk assessments "of the severity and probability of their services" causing, among other things, negative effects on civic discourse, electoral processes, or public security.[9] There is also a Code of Practice on Disinformation which was updated in 2022 which suggests a series of actionable steps that online platforms can implement to show adherence to the Digital Services Act.[10]

c. Critical Infrastructure

Securing critical infrastructure is another priority highlighted by the Europeans. A study in 2022 revealed that Germany relies on Chinese technology for 59 percent of its 5G networks.[11] Since then, there has been a movement to reduce reliance on Chinese technologies for telecommunications, as well as block Chinese companies from investing in other critical infrastructure. In 2023, the German government pushed back on Chinese investment in a Hamburg port and blocked a takeover of chips plant.[12]

The Europeans have also passed regulation to secure other facets of their critical infrastructure. One such regulation is the Digital Operational Resilience Act which seeks to enhance the IT security of financial entities, including banks, insurance companies, and investment firms. The objective is to ensure that Europe's financial sector remains resilient in the face of significant operational disruptions. Another is the EU Cybersecurity Act which creates a cybersecurity certification system for products and services.

Part III.
India's Cyber Priorities

While the Europeans focus more on establishing frameworks to address security concerns, India is more concerned with the practical aspects of cybersecurity. According to Basu (2023) much of India's focus is on shoring up domestic cybersecurity resilience and building capacity".[13] Overall, our discussions reflected this position.

a. Bolster CERT-IN

Stakeholders representing the Indian side indicated the need for bolstering the capacity of the Computer Emergency Response Team (CERT-in), the nodal Indian agency for dealing with cybersecurity incidents. This includes increased CERT-to-CERT cooperation. India also supports the creation of a standard for incident response.

b. Inter-Agency Cooperation

Some participants indicated the need to share threat intelligence and smooth out procedures for inter-agency coordination across borders.

c. Tie-in Market Access and Cyber Goals

Finally, India also sees the need to bolster cybersecurity systems as a potential market access lever. Illustratively, the industry representative at the discussion indicated that India could serve as an important partner for countries seeking secure software development.

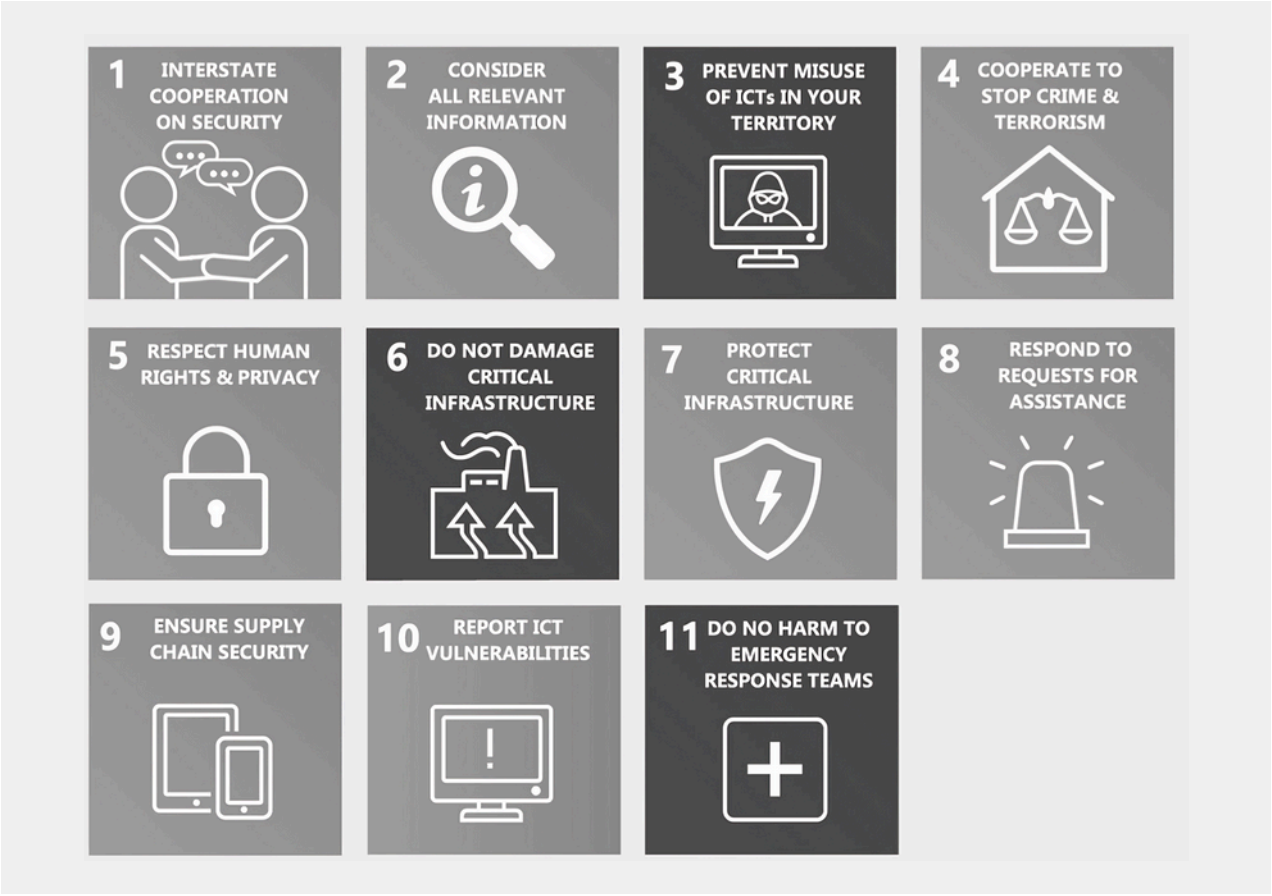
Part IV.
India and the European Union: Where they Align in Matters of Cyber Diplomacy

a. UN Norms on Responsible State Behaviour in Cyberspace

Pursuant the General Assembly resolution 68/243 in 2013, which considered information and communication technologies in the context of international security, the Secretary General of the UN established a group of governmental experts in 2014.[14] This group was formed on the basis of equitable geographical distribution. Its purpose was to continue studying, with the goal of promoting common understandings, existing and potential threats in the sphere of information security. The group also explored possible cooperative measures to address these threats. These measures included norms, rules, or principles of responsible behaviour of States, as well as confidence-building measures. Additionally, the group examined the issues of the use of information and communications technologies (ICTs) in conflicts and how international law applied to the use of ICTs by States. Furthermore, it looked into relevant international concepts aimed at strengthening the security of global information and telecommunications systems.[15]

In 2015, the group of governmental experts issued a report where it recommended a set of "voluntary, non-binding norms, rules or principles of responsible behaviour of states aimed at promoting an open, secure, stable, accessible and peaceful ICT environment".[16] Figure 1 provides an overview of these norms.

Figure 1: UN norms of responsible state behaviour in cyberspace



Through resolution 73/27, the UN General Assembly decided to form an open-ended working group (OEWG) comprising of all interested UN-member states to, in part, continue the work of the GGE on cybersecurity cooperation in 2019. In 2021, the OEWG issued a report that reaffirmed the 11 principles for responsible State behavior set forth in the 2015 GGE report. All UN member states, including the European Union and India, approved the norms.

In addition to their agreement on the UN Norms, both the Indian and European participants of our roundtable also agreed on security concerns presented by social media and the need to bolster cybersecurity within their respective jurisdictions. India aims to include content, behaviour, and speech on social media and the wider internet within the realm of international cybersecurity. In discussions on cyber/information security, India has consistently highlighted issues such as cyber terrorism, terrorist content, virulent propaganda, incitement, disinformation, terror financing, recruitment activities, and the general misuse of social media.[17]

In addition, Indian interventions have strongly emphasised the supply chain security of ICT products and services, focusing on two main aspects – enhancing cybersecurity resilience and hygiene among SMEs and children, and greater international cooperation regarding trusted ICT products and services, and reliable suppliers. This includes addressing the risk of harmful hidden functions, such as backdoors, in ICT products and services that could compromise essential networks.[18]

Part V.
Where the European Union and India Differ on Cybersecurity and Trade

Participants indicated that India and the European Union seemingly differ on the future of cyber diplomacy. In 2025, the tenure of the UN cyber diplomacy working group comes to a close.[19] In terms of the future of cyber diplomacy, there are two proposals. The first is Russia's proposal for a UN Convention on Ensuring International Information Security. The proposal advocates for sovereign equality, the territorial integrity of states, and non-interference in the internal affairs of other nations through propaganda or other means.[20] However, it has been criticised for deprioritising human rights and also for its hypocrisy, given Russia's continued influence operations across different jurisdictions.[21]

The second is the Franco-Egyptian proposal for an UN Programme of Action on Responsible Behavior in Cyberspace. The proposal is a "Programme of Action" which could create a framework and a political commitment' based on the existing international framework, i.e., recommendations, norms, and principles already agreed (referred to as *acquis*).

Now, Europe supported the Franco-Egyptian proposal but rejected the Russian one. India voted in favour of both proposals.

Other points of differentiation between the two jurisdictions include the fact that while the European agenda around cybersecurity centered primarily on normative considerations, the Indian priorities appear to be tactical. India is more concerned about the process of intelligence sharing and coordination between agencies, as these have stymied its investigative efforts in the past. Europe, on the other hand, focuses on developing frameworks and establishing global support for its normative positions. Overall, in the context of cybersecurity, India's approach seems to be more pragmatic and feasible, and is less likely to grate against the sovereignty of other countries.

Part VI.
The Way Forward

In terms of a road ahead, the EU and India must carry forward the program of action while creating channels of cooperation that better facilitate inter-agency cooperation between the two jurisdictions. This could be in the form of an executive agreement similar to those that can be formed under the US CLOUD Act. There is consensus on this topic As per the GGE 2015 recommendations, "states should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies".

Nations can also work together to put out joint-threat advisories, similar to what Europe is doing with the Republic of Korea. Essentially these advisories apprise institutions and agencies in both jurisdictions about threat actors and activities.

Endnotes

1 Chimene I. X Keitner t & Harry L. (2019) Cybersecurity Provisions and Trade Agreements, Harvard Business Law Review, Available at:https://repository.uchastings.edu/faculty_scholarship/1762

2 Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Available at: https://link.springer.com/article/10.1007/s13347-020-00423-6#citeas

3 Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Available at: https://link.springer.com/article/10.1007/s13347-020-00423-6#citeas

4 Please see Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU; Longo (2020), The Immuni app changes. It will follow the decentralized model of Apple and Google Available at: https://www.ilsole24ore.com/art/l-app-immuni-cambia-seguira-modello-decentralizzato-apple-e-google-ADcBF4L ; Busvine and Rinke (2020) Available at: Germany flips to Apple-Google approach on smartphone contact tracing)

5 Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Available at: https://link.springer.com/article/10.1007/s13347-020-00423-6#citeas

6 Sustainable Computing Lab, Vienna University of Economics and Business(2021, The 2021 German Federal Election on Social Media: An Analysis of Systemic Electoral Risks Created by Twitter and Facebook Based on the Proposed EU Digital Services Act, Available at: https://www.sustainablecomputing.eu/wp-content/uploads/2021/10/DE_Elections_Report_Final_17.pdf

7 Helena Carrapico & Benjamin Farrand (2020) Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy, Available at: https://www.tandfonline.com/doi/pdf/10.1080/07036337.2020.1853122

8 European Commission (2023) Fighting disinformation and dissemination of illegal content in the context of the Digital Services Act and in times of conflict - Speech by Commissioner Breton Available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_23_5126

9 Siren Associates (2023) Tackling disinformation: the EU Digital Services Act explained Available at: https://sirenassociates.com/policy-papers/the-eu-digital-services-act-overview-and-opportunities/

10 Siren Associates (2023) Tackling disinformation: the EU Digital Services Act explained Available at: https://sirenassociates.com/policy-papers/the-eu-digital-services-act-overview-and-opportunities/

11 Politico (2022) Germany is (still) a Huawei hotspot in Europe, Available at: https://www.politico.eu/article/germany-is-still-a-huawei-hotspot-in-europe-5g-telecoms-network/

12 Politico (2023) How China's Huawei spooked Germany into launching a probe Available at: https://www.politico.eu/article/what-trigger-germany-huawei-scare-energy-bundestag/

13 Arindrajit Basu (2023) Chapter 9: India's "passive" multistakeholder cyber diplomacy Available at: https://www.elgaronline.com/edcollchap-oa/book/9781035301546/book-part-9781035301546-16.xml

14 Summarised from UN General Assembly (2015), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf?token=f68eL09vDZMCivdZeW&fe=true

15 Summarised from Centre for Communication Governance, NLU Delhi (2021) (Cyber Security at the UN: Where Does India Stand? (Part 2) Available at https://ccgnludelhi.wordpress.com/2021/12/30/cyber-security-at-the-un-where-does-india-stand-part-2/#:~:text=This%20is%20evident%20from%20both,based%20pathway%20to%20international%20cybersecurity.

16 Bart Hogeveen(2022), The UN norms of responsible state behaviour in cyberspace, Available at: https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

17 Summarised from Centre for Communication Governance, NLU Delhi (2021) (Cyber Security at the UN: Where Does India Stand? (Part 2) Available at https://ccgnludelhi.wordpress.com/2021/12/30/cyber-security-at-the-un-where-does-india-stand-part-2/#:~:text=This%20is%20evident%20from%20both,based%20pathway%20to%20international%20cybersecurity.

18 Summarised from Centre for Communication Governance, NLU Delhi (2021) (Cyber Security at the UN: Where Does India Stand? (Part 2) Available at https://ccgnludelhi.wordpress.com/2021/12/30/cyber-security-at-the-un-where-does-india-stand-part-2/#:~:text=This%20is%20evident%20from%20both,based%20pathway%20to%20international%20cybersecurity.

19 Digiwatch (2024), UN OEWG, Available at: https://dig.watch/processes/un-gge#:~:text=%2D%20Establishment%20of%20the%20Second%20UN,2025%2C%20with%20the%20same%20mandate

20 Valentin Weber (2023) The Dangers of a New Russian Proposal for a UN Convention on International Information Security, Available at: https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security

21 Valentin Weber (2023) The Dangers of a New Russian Proposal for a UN Convention on International Information Security, Available at: https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security

About the Author

Meghna Bal is Director of the Esya Centre and an Advisor to Koan.

Acknowledgment

The author would like to thank Chhavi Pathak for her research assistance on this paper.

Disclaimer

The views expressed in this publication are not necessarily those of Friedrich-Ebert-Stiftung or of Koan Advisory

Imprint

Responsible:
Christoph Mohr I Country Director
Nithya Kochuparampil I Program Advisor, Peace and Security

T: + 91 11 26561361-64
www.india.fes.de
FriedrichEbertStiftungIndia

To order publication:
info@fes-india.org

Friedrich-Ebert-Stiftung (FES) is a non-profit German foundation, committed to the values of democracy and social justice. It was founded in 1925 and is named after Germany's first democratically elected President, Friedrich Ebert. FES India, established in the 1980s, is committed to building platforms of mutual trust for open debate and the exchange of new ideas. Using workshops, seminars, exchange programmes, and academic papers, FES India offers nuanced socio-economic analyses and furthers the debate on a national, regional and global level.

https://india.fes.de/